

Test Procedure for §170.302 (o) Access Control

This document describes the draft test procedure for evaluating conformance of complete EHRs or EHR modules to the certification criteria defined in 45 CFR Part 170 Subpart C of the Interim Final Rule (IFR) as published in the Federal Register on January 13, 2010. The document is organized by test procedure and derived test requirements with traceability to the normative certification criteria as described in the Overview document located at http://healthcare.nist.gov/docs/TestProcedureOverview_v1.pdf. These test procedures will be updated to reflect the certification criteria defined in the ONC Final Rule.

Note: This test procedure is scoped only to the criteria defined in 45 CFR Part 170 Subpart C of the Interim Final Rule (IFR) as published in the Federal Register on January 13, 2010. This test procedure will be updated to reflect updates to the criteria and standards as published in the ONC Final Rule. Questions about the criteria and standards should be directed to ONC.

CERTIFICATION CRITERIA

§170.302(o) Access Control: Assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information.

INFORMATIVE TEST DESCRIPTION

This section provides an informative description of how the test procedure is organized and conducted. It is not intended to provide normative statements of the certification requirements.

This test evaluates the capability for a Complete EHR or EHR Module¹ to assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information. The Vendor supplies the test data for this test procedure.

This test procedure consists of one section:

- Assign unique name/number – evaluates the capability to assign a unique name and/or number to track user identity and establish controls for authorized users to access electronic health information in the EHR.
 - Tester shall create a unique name/number
 - Tester shall perform authorized actions based on user permissions and verify that authorized actions were performed
 - Tester shall perform unauthorized actions and verify that the unauthorized actions were not performed

¹ Department of Health and Human Services, 45 CFR Part 170 Proposed Establishment of Certification Programs for Health Information Technology, Proposed Rule, March 10, 2010.

REFERENCED STANDARDS

None

NORMATIVE TEST PROCEDURES

Derived Test Requirements

DTR170.302.o – 1: Assign unique name/number

DTR170.302.o – 1: Assign unique name/number

Required Vendor Information

- VE170.302.o – 1.01: The Vendor shall identify the EHR function(s) that are available to assign a new user name/number, ensure that the name/number is unique, and assign permissions to the name/number for accessing electronic health information.
- VE170.302.o – 1.02: The Vendor shall identify test data necessary for this test, including a listing of existing user names/numbers.

Required Test Procedure:

- TE170.302.o – 1.01: The Tester shall identify an existing user name/number
- TE170.302.o – 1.02: Using the Vendor-identified EHR function(s), the Tester shall select an existing user name/number and shall attempt to create a duplicate user name/number
- TE170.302.o – 1.03: The Tester shall verify that the duplicate user name/number is not created
- TE170.302.o – 1.04: Using the Vendor-identified EHR function(s), the Tester shall create a unique user name/number and assign permissions to this new account to access electronic health information
- TE170.302.o – 1.05: The Tester shall verify that the unique user name/number is created
- TE170.302.o – 1.06: The Tester shall perform an action authorized by the assigned permissions
- TE170.302.o – 1.07: The Tester shall verify that the authorized action was performed
- TE170.302.o – 1.08: The Tester shall perform an action not authorized by the assigned permissions
- TE170.302.o – 1.09: The Tester shall verify that the unauthorized action was not performed

Inspection Test Guide

- IN170.302.o – 1.01: Tester shall verify that a unique user name/number has been created
- IN170.302.o – 1.02: Tester shall verify that authorized actions were performed
- IN170.302.o – 1.03: Test shall verify that unauthorized actions were no performed

TEST DATA

Test data for this test procedure is supplied by the Vendor.

CONFORMANCE TEST TOOLS

None